УДК 343

М. Н. Минисламов

преподаватель кафедры криминалистики
Сибирского юридического института МВД России
(Россия, Красноярск)

ИНТЕРНЕТ КАК СРЕДСТВО СОВЕРШЕНИЯ КИБЕРПРЕСТУПЛЕНИЙ

В настоящее время в качестве одного из главных направлений обеспечения государственной и общественной безопасности объявлено «совершенствование правового регулирования предупреждения преступности (в том числе в информационной сфере), коррупции, терроризма и экстремизма, распространения наркотиков и борьбы с такими явлениями» (п. 44 Стратегии национальной безопасности Российской Федерации) [1].

Новые возможности, которые предоставляют информационные технологии, их широкая распространенность и доступность делают эту область чрезвычайно привлекательной для представителей криминальных структур, а динамичное развитие IT-технологий, создание многочисленных информационных ресурсов и баз данных, разработка более совершенных устройств создают условия, облегчающие совершение преступлений в этой сфере, число которых в России с каждым годом увеличивается.

Российское уголовное право оказалось не достаточно готовым к стремительному развитию компьютерной техники, информационных технологий. Всемирная сеть Интернет — весьма удобная площадка для подготовки и осуществления информационно-террористических и информационно-криминальных действий. В интернет-среде могут распространяться пропагандистские материалы преступных организаций, рецепты изготовления наркотических и психотропных веществ, информация о трудоустройстве в преступные группы, о местах закладок наркотических средств и способах их оплаты и т. п. Вся эта информация легко маскируется. Отсутствие географических границ, трудно определяемая национальная принадлежность объектов Сети, возможность анонимного доступа к ее ресурсам — все это делает уязвимыми системы общественной и личной безопасности.

Результаты социологических опросов, проводимых в России, позволяют охарактеризовать активность общества в виртуальном пространстве как рискогенное, сопряженное с наличием ряда опасностей и угроз. Следует отметить, что интернет-среда продуцирует опасные для психического здоровья, репутации и материального благосостояния общества негативные явления. Среди опрошенных присутствует доля тех, кто имеет некоторое представление об опасности попадания под чужое влияние в интернет-среде, а также часть респондентов полагает, что некоторые информационные ресурсы проводят формирование нужного владельцам этого ресурса общественного мнения, поведенческих установок, мировоззрения. Это относится, по мнению опрошенных, к Facebook (43,2 % респондентов), Yandex (34,3 %), Google (31,4 %), Telegram (28,4 %). Как известно, опасность превращается в реальную угрозу, если человек и общество не могут противостоять ей [2, с. 27].

С 2013 по 2016 год число преступлений, совершаемых с использованием интернета и коммуникационных устройств, увеличилось с 11 до 66 тысяч. В 2017 году наблюдается значительный рост киберпреступлений: их число достигло 40 тысяч. В список основных источников кибератак в России по-прежнему входят собственные сотрудники (77 %), криминальные синдикаты (54 %), а также хакеры-одиночки (37 %). Мнение российских респондентов относительно источников кибератак коррелирует с мнением респондентов по всему миру (Отчет Group-IB «Hi-tech crime trends 2016»).

Генпрокурор Российской Федерации Юрий Чайка отметил, что в России большое распространение имеют кибермошенничество, информационные блокады, компьютерный шпионаж, незаконный оборот наркотических средств и другие посягательства, представляющие повышенную опасность для общества. В 2016 году в России две трети преступлений экстремистской направленности и каждое девятое преступление террористического характера совершены с использованием сети Интернет.

Значительное число киберпреступлений связано и с оборотом наркотических средств. Все чаще распространители наркотиков переходят на бесконтактный способ их сбыта, следовательно, киберпреступность в экономической и социальной сфере будет продолжать расти. Так, по данным ГУКОН МВД России, в первом полугодии 2017 года было выявлено 3 775 преступлений, связанных с

незаконным оборотом наркотиков, совершенных с использованием IT-технологий, к уголовной ответственности привлечено 1583 лица. Из незаконного оборота изъято свыше 760 кг наркотиков, пресечена деятельность 1 345 интернет-ресурсов, посредством которых осуществлялась торговля наркотиками. На территории Российской Федерации решением Роскомнадзора доступ к ним запрещен.

В 2016 году на пленарной сессии «Киберпреступность — одна из ключевых угроз роста мировой экономики. Готова ли Россия к новым вызовам?» в г. Сочи были озвучены следующие прогнозы: количество киберпреступлений в России к 2018 году может вырасти примерно в четыре раза, а общие потери страны от них могут превысить 2 триллиона рублей. По словам модератора сессии зампреда Сбербанка Станислава Кузнецова, «в России сейчас бум диджитализации, и как следствие, Россия находится в числе главных целей киберпреступников» [3]. Чтобы защититься от хакеров, в экономически развитых странах резко увеличиваются затраты на кибербезопасность, а в настоящее время в России даже нет ответственности за фишинг и спам, а максимальное наказание, которое предусмотрено действующим законодательством, не превышает семи лет лишения свободы, и штраф в 500 тысяч рублей. В США, например, за эти правонарушения можно получить до 25 лет (Путь к киберустойчивости: прогноз, защита, реагирование : 19-е международное исследование EY в области информационной безопасности за 2016–2017 годы).

В ходе дискуссий и обсуждений представителями власти и силовых структур были предложены меры, которые, по их мнению, необходимо предпринять для изменения ситуации. В первую очередь, необходимо определить, кто станет координировать такую работу со стороны федеральных структур и кредитных организаций. Следует также усилить законодательную базу, организовать подготовку специалистов в данной области, на телевидении и других СМИ рассказывать гражданам о существующей опасности (т. е. развивать «киберкультуру»), усилить государственное регулирование в этой области для организаций, которые занимаются финансовыми операциями.

Динамика диджитализации и технологической цифровой революции такова, что темпы совершенствования законодательства должны быть принципиально иными. В законодательной базе

должна быть предусмотрена ответственность за преступления в сфере информационных технологий, уточнены полномочия органов власти, для того чтобы каждый гражданин понимал, куда обращаться и как наиболее эффективно добиться расследования киберпреступлений и преследования злоумышленников. Если не решать эти вопросы, последствия нашей цифровизации негативно скажутся на экономике России [4]. В июне 2016 года Министерство внутренних дел Российской Федерации, Федеральная служба безопасности, Банк России, а также Минкомсвязь озвучили, что ведут соответствующую работу и в ближайшее время появится целый ряд законодательных инициатив, которые позволят усилить борьбу с киберпреступностью [5].

Современное развитие IT-технологий характеризуется непрерывным ростом преступлений и других общественно опасных деяний посредством Всемирной сети, что подтверждено официальной статистикой и научными исследованиями как в России, так и за рубежом. Учитывая эту негативную тенденцию в области правовой борьбы с преступностью в сети Интернет, необходимы решительные меры по противодействию и профилактике данного вида преступлений криминологического и уголовно-правового характера.

Таким образом, проблема преступности в Глобальной сети является одной из главных составляющих информационной безопасности Российской Федерации, относится к актуальным, своевременным, имеющим теоретическое и практическое значение.

Список основных источников

1. О Стратегии национальной безопасности Российской Федерации [электронный ресурс] : Указ Президента РФ, 31 дек. 2015 г., № 683 : в ред. Указа Президента РФ от 31.12.2015 г. // Собрание законодательства РФ / Официальный интернет-портал правовой информации. — М., 2015.

2. Кибакин, М. В. Студенческая молодежь в виртуальном пространстве: опасности и риски / М. В. Кибакин, П. В. Разов // Дайджест научной жизни Финуниверситета. — 2017. — № 3. — С. 27–29.

3. Гайфутдинов, Р. Р. К вопросу о типологии личности компьютерных преступников с учетом характера и мотивации их криминальной деятельности / Р. Р. Гайфутдинов // Вопросы российского и международного права. — 2017. — Т. 7, № 4А. — С. 245–256.

4. Интернет-портал Российской газеты [Электронный ресурс] / Российская газета. — Режим доступа: https://www.rg.ru. — Дата доступа: 03.11.2017.

5. Интернет-портал Минкомсвязь России [Электронный ресурс] / Минкомсвязь России. — Режим доступа: http://www.minsvyaz.ru. — Дата доступа: 30.10.2017.

УДК 343.98+004.7

В. В. Молоков
начальник кафедры информационно-правовых дисциплин
и специальной техники
Сибирского юридического института МВД России,
кандидат технических наук, доцент

ОРГАНИЗАЦИЯ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ

Одной из актуальных проблем масштабной информатизации государственной, экономической, социальной сфер общества и частной жизни человека является угроза противоправных деструктивных действий, исходящая со стороны пространства сети Интернет. Это прежде всего преступления, связанные с мошенничеством, кибератаками, схемами нелегального бесконтактного сбыта наркотиков, экономическими преступлениями и т. п. К сожалению, все эти факты являются обратной стороной технологического прогресса. Это не может не вызывать озабоченности государства и, как следствие, усиления мер противодействия преступлениям, совершаемым посредством сети Интернет [1]. Важную роль в борьбе с такого рода преступлениями занимают правоохранительные органы и органы государственной безопасности.

Выделим факторы, способствующие совершению преступлений с использованием сети Интернет:

Огромная популярность Всемирной паутины и интернет-сервисов.

Наличие средств анонимизации пользователей в сети. Использование анонимных прокси-серверов, VPN-туннелей, децентрализованных сетей типа Tor.

Широкое применение методов криптографии.

Популярность криптовалют и технологий блокчейн.